Journal of Symbolic Computation 44 (2009) 1212–1222

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Separating invariants

Gregor Kemper [1]

Technische Universität München, Zentrum Mathematik - M11, Boltzmannstr. 3, 85748 Garching, Germany

ARTICLE INFO

Article history:
Received 21 September 2007
Accepted 22 February 2008
Available online 13 February 2009

Dedicated to the memory of Karin Gatermann

Keywords:
Invariant theory
Noether's degree bound
Separating subsets

ABSTRACT

This paper studies separating subsets of an invariant ring or, more generally, of any set consisting of functions. We prove that a subset of a finitely generated algebra always contains a finite separating subset. We also show that a general version of Noether's degree bound holds for separating invariants, independently of the characteristic. While the general finiteness result is non-constructive, the Noether bound provides an easy algorithm for computing separating invariants of finite groups. The paper also contains a conceptual investigation of the difference between separating and generating subsets.

© 2009 Elsevier Ltd. All rights reserved.

0. Introduction

The main objects of interest in invariant theory are invariant rings of finite or algebraic groups. One of the classical problems is the computation of generating subsets of invariant rings. This is a difficult task, which in almost all cases involves Gröbner basis computations. In other cases, finite generating subsets do not exist at all, and there are still a range of cases where finite generating subsets exist, but we do not have algorithms for computing them. For an overview on these topics, we refer the reader to the book by Derksen and Kemper (2002). Another main topic in invariant theory is separating properties of invariants, i.e., the question of which group orbits can be separated by invariants.

A few years ago, a new trend emerged, which combines the two aspects mentioned above. Instead of considering (and being obsessed with) generating subsets, one considers sets of invariants which have exactly the same separating capabilities as the invariant ring as a whole. This concept is made precise (in a much more general context) in Definition 1 of this paper. The concept of separating subsets is a weakening of the concept of generating subsets. Therefore it is reasonable to hope that separating invariants may be better behaved than generating ones.

E-mail address: kemper@ma.tum.de.
URL: http://www-m11.ma.tum.de/~kemper.
[1] Tel.: +49 89 289 17454; fax: +49 89 289 17457.

0747-7171/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.02.012

The idea of using separating invariants is very natural. It is also very suitable for applications. In fact, applications of invariant theory to such areas as computer vision (Mundy and Zisserman, 1992), graph theory (Thiéry, 2000), orbit space reduction (Gatermann, 2000), and geometric classification (Boutin and Kemper, 2004) all rely on separating properties of invariants. Therefore, using separating invariants is much more appropriate for these applications than using generating invariants. Separating invariants are also of relevance in computational invariant theory. In fact, we have an algorithm for computing separating invariants of reductive groups acting on affine varieties (see Kemper (2003)). In the same paper, this algorithm is combined with the observation that in the case of a linear action on a vector space, the gap between separating and generating invariants can be bridged algorithmically. This combination yields an algorithm for computing generating invariants of reductive groups acting linearly on finite-dimensional vector spaces, where separating invariants provide an important intermediate step. This was recently extended further by Derksen and Kemper (2008), who gave an algorithm for computing generating invariants of a reductive group acting on an affine variety.

The following results indicate that separating invariants are indeed better behaved than generating ones, especially when one considers the *modular case*, i.e., the case of positive characteristic dividing the group order, if the group is finite.

(1) Every invariant ring has a finite separating subset (see Derksen and Kemper (2002, Theorem 2.3.15)). In contrast, not all invariant rings have finite generating subsets. (The first such examples were found by Nagata (1959), thus providing counter-examples to Hilbert's fourteenth problem.)
(2) For finite groups acting linearly on finite-dimensional vector spaces, Noether's degree bound always holds for separating invariants, i.e., there exist homogeneous separating invariants of degree at most the group order (see Derksen and Kemper (2002, Corollary 3.9.14)). But for generating invariants, the Noether bound is often violated in the modular case (see the remark after the proof of Corollary 24 in this paper).
(3) An important classical tool in invariant theory is Weyl's polarization theorem, which says the following: Let G be a group acting linearly on an n-dimensional vector space V, and let S be a generating subset of the ring $K[V^n]^G$ of vector invariants of n copies of V (with V^n standing for the direct sum of n copies of V with diagonal G-action). Then polarizing the elements of S yields a generating subset of the ring $K[V^m]^G$ of vector invariants of any number of copies. But this theorem only holds if $\operatorname{char}(K) = 0$, and fails in positive characteristic. The question is what happens when one substitutes "generating" by "separating" in Weyl's theorem. The answer was recently given by Draisma et al. (in press), who proved that Weyl's theorem holds for separating invariants, independently of the characteristic.
(4) Along similar lines, the following nice result was obtained by Domokos (2007): If G acts linearly on an n-dimensional vector space V, then for each m there exist separating invariants in $K[V^m]^G$ each of which depend only on at most $2n$ of its m arguments. An even better result holds if G is reductive.

In this paper, we add further substance to the claim that separating subsets are better behaved than generating ones. We do that by generalizing the results mentioned in (1) and (2) above. We prove that any subset $F \subseteq A$ of a finitely generated algebra A of functions has a finite separating subset (see Theorem 12). The finiteness result mentioned in (1) appears as the (very) special case that F is the invariant ring of some group. Our proof is highly inconstructive. In contrast, we give a completely constructive method for converting a finite separating subset $\{f_1, \ldots, f_n\}$ of a set F of functions into a finite separating subset of the set F^G of invariants, provided the f_i all have finite G-orbits (see Theorem 16). This algorithm only requires arithmetic operations in a finitely generated algebra (in the standard case, a polynomial algebra), and is, in particular, Gröbner basis-free. The algorithm implies a very general version of the "relative" Noether bound (see Corollaries 23 and 24), which is independent of the characteristic. By counting the separating invariants obtained from our algorithm, we find upper bounds for the number of separating invariants (see Corollary 19). It may come as a surprise that these bounds are significantly lower than the minimal numbers of generating invariants for some examples.

A further goal of this paper is to shed some light on the conceptual differences between separating and generating subsets. We do this by interpreting the concept of "separating" as "generating in a different way" (see Theorem 10 (c)). This result is stated in terms of the functional hull, which we introduce in Definition 6. The functional hull is a closure operation in the same way as generation as groups or as algebras, or formation of a convex hull are closure operations (see Proposition 9). We also show that in the theory of functionally closed sets, subobjects of finitely generated objects are always finitely generated (Corollary 11).

Considering so much evidence for the good behavior of separating invariants, one wonders whether separating invariants also have better structural properties than generating ones. In Example 5, we see a separating subalgebra which is a hypersurface, whereas the complete invariant ring is not even Gorenstein. Do all invariant rings have such nice separating subalgebras? If it is true that all defects of modular invariant theory go away when considering separating invariants instead of generating ones, then every invariant ring should have a separating subalgebra that is Cohen–Macaulay. Unfortunately, to date almost nothing is known about these questions. In particular, we do not know of any example of an invariant ring which is not Cohen–Macaulay, but which has a separating subalgebra which is Cohen–Macaulay. But neither do we have an example where we know for sure that such a separating subalgebra does not exist.

1. Separating and generating subsets

Everything in this paper is built on the following definition.

Definition 1. Let X and K be sets. We write K^X for the set of all functions from X to K. Let $F \subseteq K^X$. A subset $S \subseteq F$ is called *F-separating* if for all $x, y \in X$ we have:

$$\text{If } f(x) = f(y) \text{ for all } f \in S, \text{ then } f(x) = f(y) \text{ for all } f \in F.$$

In other words, a separating subset S is a subset of F which has the same capabilities of separating points from X as F itself: If two points can be separated by a function from F, i.e., if the function takes different values at these points, then they can also be separated by a function from S. In the context of this paper, the main interest lies in the case where F is the invariant ring of a group acting on a vector space or a variety X over a field K. But we first consider a general example.

Example 2. Assume that K contains at least two distinct elements a, b. For $y \in X$ define

$$\delta_y \colon X \to K,\ x \mapsto \begin{cases} a & \text{if } x = y \\ b & \text{if } x \neq y. \end{cases}$$

Then $S := \{\delta_y \mid y \in X\}$ is K^X-separating.

Every set $F \subseteq K^X$ of functions $X \to K$ induces an equivalence relation $\sim_F$ on X, defined by saying $x \sim_F y$ for $x, y \in X$ if $f(x) = f(y)$ for all $f \in F$. A subset $S \subseteq F$ is F-separating if and only if the relations $\sim_S$ and $\sim_F$ coincide. The following proposition shows that the restriction that S be a subset of F is essential, since without that restriction very small separating sets would often exist (see Example 4).

Proposition 3. *Let X and K be sets and $S \subseteq K^X$ a set of functions. Let $\approx$ be an equivalence relation that is coarser than $\sim_S$ (i.e., $x \sim_S y$ implies $x \approx y$). Then there exists a subset $T \subseteq K^X$ whose cardinality is less than or equal to the cardinality of S, such that T induces $\approx$.*

Proof. We write $\sim$ for $\sim_S$, and $X/\!\sim := \{[x]_\sim \mid x \in X\}$ for the set of equivalence classes. The map

$$\Phi \colon X \to K^S \quad \text{with } \Phi(x) \colon S \to K,\ f \mapsto f(x) \quad \text{for } x \in X$$

induces an injection $X/\!\sim \hookrightarrow K^S$. Since $X/\!\approx$ has cardinality less than or equal to the cardinality of $X/\!\sim$, it follows that there also exists an injection $\Psi \colon X/\!\approx \hookrightarrow K^S$. For $f \in S$, define

$$g_f \colon X \to K,\ x \mapsto \Psi([x]_\approx)(f),$$

and set $T := \{g_f \mid f \in S\}$. Clearly T has cardinality no greater than that of S. Take $x, y \in X$. It follows from the definition of g_f and from the injectiveness of Ψ that $x \approx y$ if and only if $g_f(x) = g_f(y)$ for all $f \in S$. □

Example 4. If K is of the same or greater cardinality than X (which is the case in the standard situation where K is an infinite field and X is a finite-dimensional vector space or an affine variety over K),

then there exists an injection $f\colon X \to K$, so with $S := \{f\}$ the induced relation $\sim_S$ is equality. By Proposition 3, every equivalence relation on X is induced by a single function $X \to K$.

If K is a commutative ring with unity, then K^X, equipped with pointwise operations, is an associative, commutative K-algebra with unity. If $F \subseteq K^X$ is a subalgebra generated (as an algebra) by $S \subseteq F$, then S is clearly F-separating. In other words, the concept of a separating subset is a weakening of the concept of a generating subset. This is illustrated by the following example.

Example 5. Let K be a field, $X = K^2$, and let x and y be the coordinate functions on X. Consider the functions

$$f_1 = x^3, \qquad f_2 = x^2y, \qquad f_3 = xy^2, \qquad f_4 = y^3,$$

and let $F = K[f_1, \ldots, f_4]$ be the subalgebra of K^X generated by the f_i. In fact, if $\operatorname{char}(K) \neq 3$ and K contains a primitive third root of unity ω, then F is the invariant ring of the action of the group $G = \langle\omega\rangle$ on X by scalar matrices. Consider the subset

$$S = \{f_1, f_2, f_4\}.$$

For a vector $v \in X$ with $f_1(v) \neq 0$ we have $f_3(v) = f_2(v)^2/f_1(v)$. On the other hand, $f_1(v) = 0$ implies $f_3(v) = 0$. Thus S is F-separating. However, S does not generate F as a K-algebra. In fact, there exists no generating subset of F with fewer than 4 elements.

Note that the algebra $K[S]$ generated by S is a hypersurface, whereas F is Cohen–Macaulay but not Gorenstein (and in particular not a hypersurface). So in this example we have a separating subalgebra with much better structural properties.

At this point we embark on a digression. To obtain a better understanding of the comparison between "generating" and "separating", we wish to interpret the concept of "separating" as a different nature of generation, much in the same way as we already distinguish between generation as an ideal, field extension etc. Readers who are not interested in this may choose to proceed to Section 2.

Definition 6. Let X and K be sets and $S \subseteq K^X$. Define a map

$$\Phi_S\colon X \to K^S \quad \text{by } \Phi_S(x)\colon S \to K,\ f \mapsto f(x) \quad \text{for } x \in X.$$

The *functional hull* of S is defined by

$$\langle S\rangle_{\text{func}} := \{\psi \circ \Phi_S \mid \psi\colon K^S \to K \text{ a function}\} \subseteq K^X.$$

S is called *functionally closed* if $\langle S\rangle_{\text{func}} = S$.

Example 7. Let S be the set of all constant functions $X \to K$. Then S if functionally closed. Moreover, $S = \langle\emptyset\rangle_{\text{func}}$.

If $S = \{f_1, \ldots, f_n\} \subseteq K^X$ is a finite set of functions, then the functional hull of S is easier to express by defining

$$(f_1, \ldots, f_n)\colon X \to K^n, \qquad x \mapsto (f_1(x), \ldots, f_n(x))$$

and observing that

$$\langle S\rangle_{\text{func}} := \{\psi \circ (f_1, \ldots, f_n) \mid \psi\colon K^n \to K \text{ a function}\}.$$

If K is a commutative ring and $S \subseteq K^X$, it is clear that the subalgebra $K[S]$ generated by S is contained in the functional hull $\langle S\rangle_{\text{func}}$.

Lemma 8. *Let X and K be sets, and $S \subseteq K^X$. Then we have:*

(a) $S \subseteq \langle S\rangle_{\text{func}}$.
(b) *Every constant function $X \to K$ lies in $\langle S\rangle_{\text{func}}$.*
(c) *If $T \subseteq S$, then $\langle T\rangle_{\text{func}} \subseteq \langle S\rangle_{\text{func}}$.*
(d) *$\langle S\rangle_{\text{func}}$ is functionally closed.*

Moreover, if $\mathcal{M}$ is a non-empty set of functionally closed subsets of K^X, then

$$F := \bigcap_{S \in \mathcal{M}} S$$

is functionally closed.

Proof. To prove (a), take $f \in S$ and define $\psi_f \colon K^S \to K,\ v \mapsto v(f)$. Then $\psi_f \circ \Phi_S = f$, so $f \in \langle S \rangle_{\text{func}}$. To prove (b), take $a \in K$ and define $\psi_a \colon K^S \to K,\ v \mapsto a$. Then $\psi_a \circ \Phi_S$ is the constant function $X \to K$ mapping everything to a. To prove (c), take $\rho \colon K^T \to K$ and define

$$\psi \colon K^S \to K,\ v \mapsto \rho(v|_T).$$

Let $x \in X$. Then clearly $\Phi_S(x)|_T = \Phi_T(x)$, so

$$(\psi \circ \Phi_S)(x) = (\rho \circ \Phi_T)(x),$$

and we obtain $\rho \circ \Phi_T = \psi \circ \Phi_S \in \langle S \rangle_{\text{func}}$.

The last claim about the intersection of functionally closed sets follows from (a) and (c). Indeed, $F \subseteq \langle F \rangle_{\text{func}}$ by (a), and for every $S \in \mathcal{M}$ we have $\langle F \rangle_{\text{func}} \subseteq \langle S \rangle_{\text{func}} = S$ by (c) and by the assumption; hence $\langle F \rangle_{\text{func}} \subseteq F$.

Finally, we prove (d). Set $F := \langle S \rangle_{\text{func}}$. We have $F \subseteq \langle F \rangle_{\text{func}}$ by (a). To prove the reverse inclusion, let $\rho \colon K^F \to K$ be a function. We need to produce a function $\psi \colon K^S \to K$ with

$$\rho \circ \Phi_F = \psi \circ \Phi_S. \tag{1}$$

Then $\rho \circ \Phi_F \in \langle S \rangle_{\text{func}} = F$, completing the proof. For $f \in F$ choose $\psi_f \colon K^S \to K$ with $f = \psi_f \circ \Phi_S$. For $v \in K^S$ define $w_v \colon F \to K,\ f \mapsto \psi_f(v)$. We obtain $\psi \colon K^S \to K,\ v \mapsto \rho(w_v)$. Let $x \in X$. Then for every $f \in F$, we have

$$w_{\Phi_S(x)}(f) = \psi_f(\Phi_S(x)) = f(x) = \Phi_F(x)(f),$$

so $w_{\Phi_S(x)} = \Phi_F(x)$. Thus

$$\psi(\Phi_S(x)) = \rho(w_{\Phi_S(x)}) = \rho(\Phi_F(x)),$$

and (1) follows. □

The following proposition yields an interpretation of the functional hull as a closure operation.

Proposition 9. *Let X and K be sets, and $S \subseteq K^X$. With*

$$\mathcal{M} := \left\{ F \subseteq K^X \mid F \text{ functionally closed and } S \subseteq F \right\}$$

we have

$$\langle S \rangle_{\text{func}} = \bigcap_{F \in \mathcal{M}} F.$$

Proof. This follows from (a), (c), and (d) of Lemma 8. □

Part (c) of the following theorem contains the connection between separating subsets and functional hulls.

Theorem 10. *Let X and K be sets which are not both empty, and let $S, T \subseteq K^X$ be sets of functions $X \to K$.*

(a) *The equivalence relation $\sim_T$ is coarser than $\sim_S$ (i.e., $x \sim_S y$ implies $x \sim_T y$) if and only if $T \subseteq \langle S \rangle_{\text{func}}$.*
(b) *The equivalence relations $\sim_S$ and $\sim_T$ coincide if and only if $\langle S \rangle_{\text{func}} = \langle T \rangle_{\text{func}}$.*
(c) *Assume $S \subseteq T$. Then S is T-separating if and only if $T \subseteq \langle S \rangle_{\text{func}}$.*

Proof. We start with proving (a). Assume that $\sim_T$ is coarser than $\sim_S$. Take $f \in T$. We need to show that $f \in \langle S \rangle_{\text{func}}$. Set $I := \Phi_S(X) \subseteq K^S$. For $v \in I$, choose $x \in X$ with $v = \Phi_S(x)$. Set $\psi(v) := f(x)$. This

does not depend on the choice of x. Indeed, if $v = \Phi_S(y)$ for a $y \in X$, then for every $g \in S$ we have

$$g(x) = \Phi_S(x)(g) = \Phi_S(y)(g) = g(y),$$

so $f(x) = f(y)$ by the assumption that $\sim_T$ is coarser than $\sim_S$. If $K = \emptyset$, then automatically $I = K^S$. Otherwise, we can extend ψ from I to K^S and obtain a function $\psi\colon K^S \to K$. By construction we have $\psi \circ \Phi_S = f$, so we do indeed have $f \in \langle S\rangle_{\text{func}}$.

Now assume $T \subseteq \langle S\rangle_{\text{func}}$ and take $x, y \in X$ with $x \sim_S y$. Thus $\Phi_S(x)(f) = f(x) = f(y) = \Phi_S(y)(f)$ for $f \in S$, so

$$\Phi_S(x) = \Phi_S(y). \tag{2}$$

Now let f be a function from T. By assumption, $f = \psi \circ \Phi_S$ with $\psi\colon K^S \to K$. With (2), this implies $f(x) = f(y)$. So $x \sim_T y$.

To prove (b), observe that by Lemma 8(a), (c) and (d), the condition $T \subseteq \langle S\rangle_{\text{func}}$ is equivalent to $\langle T\rangle_{\text{func}} \subseteq \langle S\rangle_{\text{func}}$. Therefore part (b) follows from (a).

To prove (c), assume that $S \subseteq T$ is T-separating. Then $\sim_S$ and $\sim_T$ coincide, so $T \subseteq \langle S\rangle_{\text{func}}$ by (a). Conversely, if $T \subseteq \langle S\rangle_{\text{func}}$, then by Lemma 8(c) and (d) we obtain $\langle S\rangle_{\text{func}} \subseteq \langle T\rangle_{\text{func}} \subseteq \langle S\rangle_{\text{func}}$. By (b), this implies the coincidence of $\sim_S$ and $\sim_T$, so S is T-separating. □

In almost every algebraic theory, the question arises of whether subobjects of finitely generated objects are again finitely generated. For example, the answer is "yes" in the theory of field extensions and of vector spaces, but "in general no" in the theory of commutative algebras and of modules. The following result implies that in the theory of functionally closed sets, subobjects of finitely generated objects are indeed finitely generated.

Corollary 11. *Let X and K be sets, $S \subseteq K^X$ a set of functions, and $F \subseteq \langle S\rangle_{\text{func}}$ a subset of the functional hull of S. If F is functionally closed, then there exists a subset $T \subseteq F$ of cardinality at most the cardinality of S, such that $F = \langle T\rangle_{\text{func}}$.*

Proof. First the corollary is verified for the trivial case $K = X = \emptyset$ by some brain-twisting. Consider the general case. By Theorem 10(a), the equivalence relation $\sim_F$ induced by F is coarser than $\sim_S$. By Proposition 3, there exists $T \subseteq K^X$ of cardinality at most the cardinality of S, such that T induces $\sim_F$. By Theorem 10(b), this implies $\langle T\rangle_{\text{func}} = \langle F\rangle_{\text{func}}$, so the result follows from the closedness of F. □

2. Finiteness

It is known that subalgebras of finitely generated algebras need not be finitely generated. An example of this phenomenon is given in Example 14. The following theorem provides a first indication that separating subsets are better behaved than generating subsets. In the context of this paper, the main application is for the case where A is the ring of polynomial functions on a finite-dimensional vector space V or the ring of regular functions on an affine variety X, and F is the invariant ring of a group acting on V or on X. This special case of the theorem can be found in Derksen and Kemper (2002, Theorem 2.3.15).

Theorem 12. *Let X be a set, K a Noetherian commutative ring with unity, $A \subseteq K^X$ a finitely generated subalgebra of K^X, and let $F \subseteq A$ be subset. Then there exists a finite subset $S \subseteq F$ which is F-separating.*

Proof. The proof is amazingly simple. Consider the natural projections $\pi_1, \pi_2\colon X \times X \to X$ and define

$$\varphi_i\colon K^X \to K^{X\times X},\ f \mapsto f \circ \pi_i \quad (i = 1, 2).$$

These are homomorphisms of K-algebras. We have $A = K[g_1, \ldots, g_m]$ with $g_i \in K^X$. Let $B \subseteq K^{X\times X}$ be the subalgebra generated by all $\varphi_i(g_j)$. Then B is Noetherian, and $\varphi_i(A) \subseteq B$ for $i = 1, 2$. Let $I \subseteq B$ be the ideal generated by all $\varphi_1(f) - \varphi_2(f), f \in F$. Since B is Noetherian, there exist $f_1, \ldots, f_n \in F$ such that I is generated by $\varphi_1(f_i) - \varphi_2(f_i)$ $(i = 1, \ldots, n)$ as an ideal in B. We claim that $S := \{f_1, \ldots, f_n\}$ is F-separating. Indeed, take $x, y \in X$ with $f_i(x) = f_i(y)$ for all $i = 1, \ldots, n$. Let $f \in F$ be arbitrary. Since $\varphi_1(f) - \varphi_2(f)$ lies in I, there exist $h_1, \ldots, h_n \in B$ such that

$$\varphi_1(f) - \varphi_2(f) = \sum_{i=1}^{n} h_i\,(\varphi_1(f_i) - \varphi_2(f_i))\,.$$

Evaluating this at $(x, y) \in X \times X$ yields

$$f(x) - f(y) = \sum_{i=1}^{n} h_i(x, y)\,(f_i(x) - f_i(y)) = 0,$$

so $f(x) = f(y)$. This completes the proof. □

Note that the proof is highly inconstructive. Thus the following problem remains open.

Problem 13. Let G be an affine algebraic group over a field K acting on an affine variety X defined over the same field by a morphism $G \times X \to X$. Compute a finite, $K[X]^G$-separating set.

This problem was solved by Kemper (2003) for the case where G is reductive. The following example illustrates Theorem 12.

Example 14. Let K be an infinite field and let $A = K[x, y]$ be the algebra of polynomial functions on $X = K^2$. Then the subalgebra

$$F := K + x \cdot A = K[x, xy, xy^2, xy^3, \ldots]$$

is not finitely generated. In fact, if F were finitely generated, it would be Noetherian and therefore one could choose a finite subset $\mathcal{B}$ of $\mathcal{M} := \{xy^i \mid i \in \mathbb{N}_0\}$ such that $\mathcal{B}$ generates the F-ideal $\langle \mathcal{M} \rangle_F$ generated by $\mathcal{M}$. But this is not the case. However, Theorem 12 predicts that F has a finite separating subset. Indeed, it is easy to verify that $S = \{x, xy\}$ is F-separating.

It would be even nicer if in Theorem 12 the hypothesis that A be finitely generated as an algebra could be weakened to saying that A should have a finite separating subset. However, this is not true, as the following example shows.

Example 15. Let K be an infinite commutative ring with unity, n a positive integer, $X = K^n$, and $A = K^X$. The polynomial functions $x_1, \ldots, x_n$ form a finite, A-separating set. But it is easy to see that the subset

$$F = \{f \in K^X \mid f \text{ has finite image}\}$$

has no finite, separating subset. Note that F is itself an algebra.

This example also shows that there exist subalgebras of K^X which have no finite separating subset.

3. Finite groups

The finiteness result in Theorem 12 is highly inconstructive. In contrast, we will get a completely constructive procedure for finding separating invariants of finite groups. This procedure only requires arithmetic operations in a finitely generated algebra, which in the standard case is a polynomial algebra. We consider the following situation.

Throughout this section, let X be a set and let K be an integral domain. Let G be a group acting on X. Then G acts on K^X by automorphisms of K-algebras via

$$\sigma(f) = f \circ \sigma^{-1} \quad \text{for } \sigma \in G,\ f \in K^X.$$

Let $F \subseteq K^X$ be a subset, and write

$$F^G := \{f \in F \mid \sigma(f) = f \text{ for all } \sigma \in G\}.$$

We do not assume that F is closed under the G-action. Moreover, let $\{f_1, \ldots, f_n\} \subseteq F$ be an F-separating subset. We assume that the G-orbits of all f_i are finite. Consider the subalgebra $A := K[\sigma(f_i) \mid \sigma \in G,\ i \in \{1, \ldots, n\}] \subseteq K^X$ generated by all $\sigma(f_i)$, and assume that

$$A^G \subseteq F. \tag{3}$$

Choose a ring extension L of K such that L is an integral domain and free of rank at least n (the rank may be infinite) as a K-module. Let $\mathcal{U}$ be a K-basis of L, and let $u_1, \ldots, u_n \in L$ be linearly independent

over K. Form the set

$$M := \left\{ \sum_{i=1}^{n} u_i \otimes \sigma(f_i) \,\middle|\, \sigma \in G \right\} \subseteq L \otimes_K A,$$

which is finite. Introducing an indeterminate T, we can form the polynomial

$$g(T) = \prod_{m \in M} (T - m) \in (L \otimes_K A)[T].$$

Readers might wish to look at Remark 17 now, where the standard situation is described and some generalizations are discussed. Write

$$g(T) = T^{|M|} + \sum_{i=1}^{|M|} \left(\sum_{u \in \mathcal{U}} u \otimes a_{i,u} \right) \cdot T^{|M|-i}$$

with $a_{i,u} \in A$, and form the finite set

$$S := \{ a_{i,u} \mid i \in \{1, \ldots, |M|\},\ u \in \mathcal{U} \} \setminus K \subseteq A.$$

Theorem 16. *In the above situation, S is an F^G-separating subset of F^G. In fact, if two points $x, y \in X$ satisfy $f(x) = f(y)$ for all $f \in S$, then there exists $\sigma \in G$ such that*

$$f(y) = f(\sigma(x)) \quad \text{for all } f \in F. \tag{4}$$

Proof. We let G act trivially on L and on the indeterminate T. Then M is G-stable, so $g(T)$ is G-invariant. This implies that all $a_{i,u}$ lie in A^G. Therefore by (3), they lie in F^G, so $S \subseteq F^G$.

Let $x, y \in X$ such that $a_{i,u}(x) = a_{i,u}(y)$ for all i and u. We need to show (4), and that $f(x) = f(y)$ for all $f \in F^G$. By assumption,

$$\prod_{m \in M} (T - m(x)) = \prod_{m \in M} (T - m(y)),$$

where x and y are always substituted into the second tensor factor. This is a polynomial identity in $L[T]$. Since L is an integral domain and $\sum_{i=1}^{n} u_i \otimes f_i \in M$, there exists a $\sigma \in G$ with

$$\sum_{i=1}^{n} u_i f_i(y) = \sum_{i=1}^{n} u_i \sigma(f_i)(x).$$

With the linear independence of $u_1, \ldots, u_n$, this yields

$$f_i(y) = \sigma(f_i)(x) = f_i\left(\sigma^{-1}(x)\right) \quad \text{for all } i = 1, \ldots, n.$$

Since the f_i are F-separating, this implies (4). Now let $f \in F^G$ be an invariant in F. Then (4) yields

$$f(y) = f\left(\sigma^{-1}(x)\right) = \sigma(f)(x) = f(x).$$

This completes the proof. □

Remark 17. The standard situation to which Theorem 16 applies is the following. Let K be an infinite field and let $X = V$ be an n-dimensional vector space. Assume that G is a finite group acting faithfully on V by linear or affine transformations. Let $F = K[V] = K[x_1, \ldots, x_n]$ be the ring of polynomial functions on V, so we can put $f_i = x_i$. Then F is closed under the G-action, and (3) is satisfied. The standard choice for L is a polynomial ring $L = K[U]$, so we can choose $\mathcal{U} = \{U^i \mid i \in \mathbb{N}_0\}$ and set $u_i := U^{i-1}$. Then $L \otimes_K A = F[U]$, and

$$g(T) = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} \sigma(x_i) U^{i-1} \right) \in F[U, T].$$

The separating set S is obtained by regarding $g(T)$ as a polynomial in T and U and extracting all coefficients. The additional statement (4) tells us that F^G separates all G-orbits, since F separates all points. The setting of Theorem 16 allows generalizations in various directions, and any combination of these generalizations:

(1) K may be an integral domain instead of a field.
(2) X may be an affine variety with a G-action by morphisms, in which case F would be chosen to be the ring of regular functions.

(3) L may be chosen as a field extension of K of degree at least n. This may drastically reduce the number of coefficients $a_{i,u}$ going into the separating set S. The cost of multiplying out the factors of $g(T)$ may also be reduced substantially.
(4) F may be the invariant ring $K[x_1, \ldots, x_n]^H$ of a subgroup $H \subseteq G$ of finite index (where G itself need not be finite). Then in general F is not closed under the G-action, but (3) is satisfied, and each element of F has a G-orbit of length at most $[G : H]$ (=the index of H in G) elements. If G is finite and we have a chain of subgroups, we may thus apply Theorem 16 successively to find F^G-separating invariants. Walking along a chain of subgroups may decrease the cost of the calculations dramatically.

Example 18. This is a continuation of Example 5, so G is the cyclic group of order 3 generated by a primitive third root of unity in K. If we take $L = K[U]$ to be a polynomial ring, we get

$$g(T) = T^3 - (x + yU)^3 = T^3 - x^3 - 3x^2yU - 3xy^2U^2 - y^3U^3,$$

so by Theorem 16, the set $\{x^3, x^2y, xy^2, y^3\}$ is $K[x, y, z]^G$-separating. This set is also generating, so nothing is gained. However, if K has an element a which is not a square in K, we can choose $L = K(\sqrt{a})$ and $u_1 = 1, u_2 = \sqrt{a}$, and now get

$$g(T) = T^3 - (x^3 + 3axy^2) - (3x^2y + ay^3)\sqrt{a},$$

so the smaller separating set

$$S = \{x^3 + 3axy^2, 3x^2y + ay^3\}$$

emerges.

By a simple count of the elements in the separating set produced by Theorem 16, we get an upper bound for the necessary size of a separating set. To formulate it, we write

$$\gamma_{\mathrm{sep}}(F) := \inf\{n | \text{ there exists a finite } F\text{-separating set of size } n\} \in \mathbb{N}_0 \cup \{\infty\}$$

for any set $F \subseteq K^X$, where we set $\inf(\emptyset) := \infty$.

Corollary 19. *Assume the situation and notation of Theorem 16.*

(a) *We have*

$$\gamma_{\mathrm{sep}}(F^G) \leq \frac{|M|(|M|+1)}{2} \cdot \gamma_{\mathrm{sep}}(F) - \frac{|M|(|M|-1)}{2}.$$

(b) *If there exists a ring extension L of K which is an integral domain and free of rank $\gamma_{\mathrm{sep}}(F)$ over K, then*

$$\gamma_{\mathrm{sep}}(F^G) \leq |M| \cdot \gamma_{\mathrm{sep}}(F).$$

If G is finite, then $|M| \leq |G|$.

Example 20. Let G be the cyclic group generated by a primitive m-th root of unity in K, acting by scalar matrices on $V = K^n$. By Corollary 19, there exists a $K[x_1, \ldots, x_n]^G$-separating subset of size at most $m(m+1)/2 \cdot n - m(m-1)/2$ or even at most $m \cdot n$, depending on the case. (In fact, the real size will be $m(n-1)+1$ or n; see Example 18). In contrast, a minimal generating subset of $K[x_1, \ldots, x_n]^G$ has size

$$\gamma\left(K[x_1, \ldots, x_n]^G\right) = \binom{n+m-1}{m},$$

which has degree m as a polynomial in n and thus becomes drastically bigger than the bounds for separating sets. We see that even in the simplest case of cyclic groups, separating invariants are much nicer than generating ones.

We now look at degrees. Degree considerations are often made with respect to a graduation. We take a more general view and assume that we have a filtration. More precisely, assume that $A \subseteq K^X$ is a *filtered algebra*, i.e., a subalgebra of K^X with K-submodules $A_d \subseteq A$ ($d \in \mathbb{N}_0$) such that

(i) $A_d \subseteq A_{d+1}$ for $d \in \mathbb{N}_0$,
(ii) $f \cdot g \in A_{i+j}$ for $f \in A_i$ and $g \in A_j$, and
(iii) $A = \bigcup_{d \in \mathbb{N}_0} A_d$.

We call *A finitely filtered* if additionally

(iv) all A_d are finitely generated as K-modules.

If $f \in A_d$, we say that f has degree at most d. Notice that every subalgebra $B \subseteq A$ is filtered by setting $B_d := B \cap A_d$ (but if K is not Noetherian, B need not be finitely filtered even if A is).

Example 21. If $A = K[f_1, \ldots, f_n]$ is finitely generated as an algebra, a finite filtration is obtained by taking A_d to be the K-submodule of A generated by

$$M_d = \left\{ \prod_{i=1}^{d} g_i \,\middle|\, g_i \in \{1, f_1, \ldots, f_n\} \right\}.$$

This filtration depends on the choice of the generators f_i.

If A is a filtered algebra, we define

$$\beta_{\mathrm{sep}}(A) := \inf\{d \in \mathbb{N}_0 \mid \text{there exists } S \subseteq A_d \text{ which is finite and } A\text{-separating}\},$$

where again we set $\inf(\emptyset) := \infty$, so $\beta_{\mathrm{sep}}(A) \in \mathbb{N}_0 \cup \{\infty\}$. In other words, $\beta_{\mathrm{sep}}(A)$ is the smallest number d such that there exist finitely many A-separating elements of degree at most d. In comparison, the "usual" beta-number $\beta(A)$ is defined by substituting "separating" by "generating". Also note that any grading on A leads to a filtration by taking A_d to be the sum of all homogeneous parts of degree up to d. Then our definitions of β and β_{sep} coincide with the ones for the graded case.

Remember that throughout this section, A is assumed to be a subalgebra of K^X that is stable under the G-action on K^X. We say that a A is *G-filtered* if $\sigma(f) \in A_d$ for every $\sigma \in G$ and $f \in A_d$.

Example 22. (a) If A is a finitely generated algebra and G is finite, we can always substitute a generating subset of A by the union of the G-orbits of the generators. With these new generators, we obtain a finitely G-filtered algebra B by using the filtration given in Example 21. This possibly enlarges A and may change the original filtration of A. In the case where $A = K[V]$ with V a KG-module, we get the usual filtration by degree.

(b) If G is an affine algebraic group and X a G-variety over an algebraically closed field K, then X can be embedded G-equivariantly into a G-module V (see Derksen and Kemper (2002, Lemma A.1.9), or Derksen and Kemper (2008, Section 1.1) for an algorithmic version). This yields a G-equivariant epimorphism $\pi\colon K[V] = K[x_1, \ldots, x_n] \to K[X]$. The $\pi(x_i)$ generate $K[X]$ as a an algebra, and the filtration formed with these generators as in Example 21 makes $K[X]$ into a finitely G-filtered algebra.

The second corollary of Theorem 16 is a generalization of Noether's degree bound, but for separating invariants.

Corollary 23. *In the situation introduced in the beginning of this section, assume that A is a G-filtered algebra, and let $H \subseteq G$ be a subgroup of finite index. Then*

$$\beta_{\mathrm{sep}}\left(A^G\right) \leq [G : H] \cdot \beta_{\mathrm{sep}}\left(A^H\right).$$

(A^G and A^H are considered with the induced filtration from A.)

Proof. Let $B = A^H$. We may assume that $d := \beta_{\mathrm{sep}}(B)$ is finite, so there exists a subset $\{f_1, \ldots, f_n\} \subseteq B_d = B \cap A_d$ which is B-separating. The G-orbit of each f_i lies in A_d and has length at most $[G : H]$. With $L := K[U]$ a polynomial ring, the set

$$M := \left\{ \sum_{i=1}^{n} \sigma(f_i) U^{i-1} \,\middle|\, \sigma \in G \right\} \subseteq A[U]$$

has at most $[G : H]$ elements. All coefficients of

$$g(T, U) = \prod_{m \in M} (T - m) \in A[U, T]$$

lie in $A_{|M|d}$. By Theorem 16, these coefficients form an A^G-separating subset. So $\beta_{\mathrm{sep}}\left(A^G\right) \leq |M|d$, which completes the proof. □

For the case where K is a field, the last statement of the following corollary appeared in Derksen and Kemper (2002, Corollary 3.9.14).

Corollary 24 (*Noether's bound for separating invariants*). *Let K be an integral domain, $G \subseteq \mathrm{GL}_n(K)$ a linear group, and $H \subseteq G$ a subgroup of finite index. Let $A = K[x_1, \ldots, x_n]$ be the ring of polynomial functions on K^n. Then*

$$\beta_{\mathrm{sep}}\left(A^G\right) \leq [G : H] \cdot \beta_{\mathrm{sep}}\left(A^H\right).$$

In particular, if G is finite, then

$$\beta_{\mathrm{sep}}\left(A^G\right) \leq |G|,$$

i.e., there exist homogeneous invariants of degree at most $|G|$ which form an A^G-separating set.

Proof. The standard filtration by degree makes A into a G-filtered algebra. Thus Corollary 23 applies and yields the first bound. A is generated in degree 1, so $\beta_{\mathrm{sep}}(A) = 1$. Thus the second bound is the special case $H = \{1\}$. If the separating set obtained from Corollary 23 is not homogeneous (in fact, it is), it can be substituted by the set of all homogeneous components of all its elements. □

What is remarkable about Corollary 24 is that it is independent of the characteristic of K. In this respect it contrasts strongly with the corresponding theorem about generating invariants, which requires that K is a field and $\mathrm{char}(K)$ does not divide $|G|$ (see Noether (1916), Fleischmann (2000), Fogarty (2001) and Derksen and Kemper (2002, Section 3.8)). In fact, the situation regarding generating invariants is so bad that if $\mathrm{char}(K)$ divides $|G|$, there exists no upper bound for $\beta\left(A^G\right)$ which only depends on $|G|$ (see Derksen and Kemper (2002, Section 3.9 and the references given there)). Let me also remark that, to the best of my knowledge, for the relative Noether bound

$$\beta\left(A^G\right) \leq [G : H] \cdot \beta\left(A^H\right),$$

we only have proofs for the cases where $|G|$ is invertible in K, or H normal and $[G : H]$ invertible in K (both from Sezer (2002)). It is widely believed that the relative Noether bound holds whenever $[G : H]$ is invertible in K.

Acknowledgements

This paper owes a lot to Karin Gatermann. In fact, I learned a lot about the use of separating properties of invariants, and in particular about orbit space reduction from conversations with her. These conversations influenced many of the ideas in this paper. I also thank Will Traves for some interesting conversations, which prompted me to start wondering about the "relative" way in which Theorem 16 is now stated. Finally, I thank the anonymous referees for their helpful comments.

References

Boutin, M., Kemper, G., 2004. On reconstructing n-point configurations from the distribution of distances or areas. Adv. Appl. Math. 32, 709–735.
Derksen, H., Kemper, G., 2002. Computational Invariant Theory. In: Encyclopaedia of Mathematical Sciences, vol. 130. Springer-Verlag, Berlin, Heidelberg, New York.
Derksen, H., Kemper, G., 2008. Computing invariants of algebraic group actions in arbitrary characteristic. Adv. Math. 217, 2089–2129.
Domokos, M., 2007. Typical separating invariants. Transform. Groups 12, 49–63.
Draisma, J., Kemper, G., Wehlau, D., 2006. Polarization of separating invariants. Canad. J. Math. (in press).
Fleischmann, P., 2000. The Noether bound in invariant theory of finite groups. Adv. Math. 156, 23–32.
Fogarty, J., 2001. On Noether's bound for polynomial invariants of a finite group. Electron. Res. Announc. Amer. Math. Soc. 7, 5–7.
Gatermann, K., 2000. Computer Algebra Methods for Equivariant Dynamical Systems. In: Lecture Notes in Mathematics, vol. 1728. Springer-Verlag, Berlin, Heidelberg.
Kemper, G., 2003. Computing invariants of reductive groups in positive characteristic. Transform. Groups 8, 159–176.
Mundy, J.L., Zisserman, A. (Eds.), 1992. Geometric invariance in computer vision. In: Artificial Intelligence. MIT Press, Cambridge, MA.
Nagata, M., 1959. On the 14th problem of Hilbert. Amer. J. Math. 81, 766–772.
Noether, E., 1916. Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. 77, 89–92.
Sezer, M., 2002. Sharpening the generalized Noether bound in the invariant theory of finite groups. J. Algebra 254, 252–263.
Thiéry, N.M., 2000. Algebraic invariants of graphs; a study based on computer exploration. SIGSAM Bull. 34, 9–20.